Privacy Impact Assessment
for the

Electronic Fingerprint System (EFS)

DHS/FEMA/PIA-034

September 24, 2013

Contact Point
J'son Tyson
Identity, Credential & Access Management Section Chief
Office of the Chief Security Officer
Federal Emergency Management Agency
(202) 646-1898

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Federal Emergency Management Agency (FEMA) Office of the Chief Security Officer (OSCO) is initiating the Electronic Fingerprint System (EFS). FEMA OCSO uses the EFS as part of the security suitability, clearance, and badging process for FEMA employees, contractors, and affiliates. FEMA is conducting a Privacy Impact Assessment (PIA) because EFS collects personally identifiable information (PII) and leverages National Protection and Programs Directorate (NPPD), Office of Biometric Identity Management's (OBIM) Automated Biometric Identification System (IDENT) to conduct background investigations.

Overview

As required by law, FEMA conducts background investigations of all applicants to ensure that these individuals meet established suitability and security standards. This includes conducting the suitability, clearance, and badging process for FEMA Permanent Fulltime (PFT) Employees, Temporary Fulltime (TFT) Employees, Cadres of On-Call Response Employees (CORE), Reserve Employees, contractors, individuals from voluntary organizations, and federal, state, local, and tribal partners working in furtherance of FEMA's mission. As part of this process, a fingerprint-based criminal history records check is required. To execute this check, FEMA currently obtains both the electronic fingerprints and other PII as required by the Federal Bureau of Investigation (FBI) to complete the investigation through its Integrated Automated Fingerprint Identification System (IAFIS).

FEMA OCSO is proposing to initiate the EFS to accomplish this process in a more efficient manner. To date, FEMA has been working exclusively with the FBI Criminal Justice Information Services Division (CJIS) to use IAFIS and the Office of Personnel Management (OPM) for credentialing services. Now, with the use of EFS, FEMA can automate, streamline, and reduce the time required to conduct background investigations to support staffing decisions by leveraging the IDENT system. Using EFS, applicant records will no longer be uploaded manually for investigation review; they are submitted electronically over DHS's *OneNet* network. This will reduce process time from days to hours. In addition, with the new EFS, there is no longer a need for manual entry of investigation result data; all result data is automated. This reduces the risk of human error and greatly improves process time.

In general, the background check process conducted by FEMA OCSO mirrors the process conducted by DHS OCSO as a whole, and is covered in DHS/ALL/PIA-014.[1] This includes the suitability, clearance, and badging process for all categories of inviduals mentioned above – including the individuals from state, local, and tribal entities, as well as volunteer organizations – that go through the security process, and who are issued Personal Identity

[1] For more information on DHS/ALL/PIA-014 Personal Identity Verification, please see: http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_dhs_piv_august2012.pdf

Verification (PIV) cards and granted access to FEMA information technology (IT) systems. Some volunteers from voluntary organizations may require access to FEMA IT systems for the purposes of coordinating resources in a disaster scenario. These specific volunteers would be issued PIV cards and are considered contractors to FEMA. For more information on the security suitability, clearance, and badging process, please refer to DHS/ALL/PIA-014 PIA. This PIA covers FEMA's use of EFS and its interactions with the IDENT system.

This PIA documents the transition from FEMA OSCO sending and receiving information from FBI CJIS's IAFIS to conducting these transactions using IDENT through the IDENT/IAFIS Interoperability. The IDENT/IAFIS Interoperability enables the two systems to seamlessly connect, communicate, and exchange information.

The FEMA is performing this transition in compliance with the DHS Memorandum signed by the Chief Information Officer (CIO) and the Screening Coordination Office (SCO) stating, "all DHS programs requiring the collection and use of fingerprints to vet individuals shall use the target biometric service as defined by the Homeland Security (HS) Enterprise Architecture." Currently, FEMA does not interface with OBIM (formerly the United States Visitor and Immigrant Status Indicator Technology [US-VISIT]) IDENT and will be a new user of the identity services provided by IDENT. FEMA is undergoing this transition in an effort to conduct biometric and associated biographic background checks and obtain both the IDENT and FBI responses for the purposes of credentialing all FEMA applicants.

EFS Process

FEMA OCSO uses the EFS as part of the security suitability, clearance, and badging process for all applicants and potential hires, including PFTs; TFTs; COREs; Reserve Employees; contractors; voluntary organizations; and federal, state, local, and tribal partners working in furtherance of FEMA's mission.

In the initial phases of the applicant suitability process, an applicant provides fingerprints for investigation purposes. The applicant first provides proper identification as outlined on the I-9 Form, "List of Acceptable Documents."[2] Once the applicant's identity is verified, his or her PII and ten-fingerprint biometric are collected by the secure Universal Registration Client (URC) station to initiate the personnel security and suitability processes. This station is connected to the secure FEMA *OneNet* Network and requires proper security credentials for access. Access to the URC is only granted to FEMA's trained security officials. Once the applicant data is collected and identity verified, the security official capturing the information submits the encrypted data to the FEMA Fingerprint Store and Forward (FPSF) server.

[2] An entire list of acceptable documents can be found on page 9 of the following: http://www.uscis.gov/files/form/i-9.pdf

The FPSF server then transmits the data in a secure IDENT Exchange Message (IXM) format over *OneNet* to the IDENT database. The data is then searched against IDENT, including the OBIM Watch Lists and criminal databases, then forwards the transaction to the FBI/IAFIS searching for potential matches with criminal records and rap sheet data. IAFIS sends its results back to OBIM. The results are sent with the IDENT results back to FEMA for processing. The FPSF server decodes the encrypted return message. FEMA personnel security representatives review the full criminal history results via a web interface to DHS's Integrated Security Management System (ISMS), as the results are automatically generated into this system from the FPSF server. ISMS is a web-based case management tool designed to support the lifecycle of DHS personnel security.[3]

Results are returned to FEMA within 24 hours. Once the IDENT/IAFIS result message is returned to FEMA from OBIM, personnel security specialists review the results in ISMS and determine proper adjudication methods for that applicant (i.e., whether the applicant meets suitability requirements). Individuals may directly correct inaccurate basic information such as address and phone number at any time after the clearance process is completed. This will be completed through a DHS website with manager approval of each change; however, during the clearance process individuals may not alter their information. They may inform the FEMA OCSO of a change in their information, but may not directly access it.

FEMA collects biometric and PII from prospective employees, contractors, and other affiliates from fixed locations as well as field locations in the same manner. For example during disasters, FEMA may hire contractors who are local to the area to facilitate and support the response. In order to screen these individuals, FEMA deploys fingerprinting units to various field locations, including joint field offices or other designated locations set up during a disaster. All fingerprinting units connect with the centralized FPSF server. Once prospective applicant data is captured on the fingerprinting unit, it is transmitted and saved to the FPSF server and is automatically deleted from the fingerprinting unit. Records relating to individuals are retained and disposed of in accordance with the appropriate General Records Schedule, approved by the National Archives and Records Administration (NARA).

Once FEMA OSCO obtains the criminal history and background check results from IDENT and CJIS, FEMA coordinates with OPM to conduct credit checks that supplement the background check information and is also considered during the adjudication process for the applicant. After initiating EFS, FEMA can automate this process by sending the criminal history results to OPM's investigative server using EFS, in which OPM can conduct a credit check on the individual. OPM then sends credit check results back to FEMA using EFS. Currently, this is a manual process in which OPM and FEMA send the information through the mail. The credit check process is an entirely separate EFS transaction from the IDENT/CJIS transaction. The

[3] For more information on ISMS, please see DHS/ALL/PIA-038 Integrated Security Management System, found here: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_isms.pdf.

OPM credit check is consistent with current security procedures and standards and is covered by the DHS/ALL/PIA-014 and the System of Records Notices (SORN) listed below in Section 1.2.

Evaluating and Mitigating PII Risks and Vulnerabilities

FEMA has taken steps to evaluate and mitigate PII vulnerabilities and risks associated with the current electronic fingerprint process. The holistic approach to resolving vulnerabilities has been to automate processes and reduce human interaction in those processes. For example, FEMA's current fingerprint capture process requires applicant data to be exported to compact discs (CD), which is a PII vulnerability that will be eliminated with the EFS. In addition, PII was previously stored on the capture station and was manually deleted by the security manager. With the new EFS, no PII is stored on the capture station, therefore further protecting PII.

The level of automation with the new EFS is also greatly enhanced. The URC can now use a card reader device that will capture applicant data automatically from a driver's license, rather than having to manually enter the license information into the system. This will improve process times, as well as decrease manual entry. The new EFS also sends results to ISMS automatically while previously all results were entered into ISMS manually.

Interagency Agreements

The EFS will operate under an Interconnection Security Agreement (ISA) between OBIM and FEMA.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

- 44 U.S.C. § 3544, "Federal Agency Responsibilities;"
- 5 C.F.R. Part 731, "Suitability;"
- 5 C.F.R. Part 732, "National Security Positions;"
- 32 C.F.R. § 147.24, "The National Agency Check;"
- Executive Order 10450, "Security Requirements for Government Employment;"
- Executive Order 12968, "Access to Classified Information;"
- Homeland Security Presidential Directive 12 (HSPD-12);
- DHS Delegation 12000, "Delegation to Designate Officers and Agents;"
- DHS Directive 121-01, "Chief Security Officer;" and

- DHS Instruction 121-01-007, "The Department of Homeland Security Personnel Security and Suitability Program."

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following DHS-wide SORNs, under the authority of the DHS OCSO, cover the information collection associated with the security background checks:

- DHS/ALL-023 DHS Personnel Security Management, 75 FR 8088, February 23, 2010;
- DHS/ALL-026 Personal Identity Verification Management System SORN, 75 FR 30301, June 25, 2009.

The OSCO SORNs are appropriate, rather than the existing DHS/US-VISIT IDENT SORN because the IDENT SORN only covers the retention and limited use of the information found in IDENT.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The EFS Security Plan (SP) has been developed as part of the initial Certification and Accreditation (C&A) Package. The initial C&A effort was completed September 2013 and the Authority to Operate (ATO) was granted in the 4th Quarter of Fiscal Year 2013.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

FEMA retains the personnel security clearance records in accordance with NARA General Records Schedule (GRS) 18, Security and Protective Services Records, items 20 through 25.

The IDENT database itself retains biometric and biographic data in accordance with Records Schedule Number DAA-0563-2013-001.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The collection of information from federal employees and contractors does not fall under the purview of PRA. FEMA/OCSO is working with the PRA program

management office to address PRA requirements related to the collection of information from members of the public.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The following PII is collected and entered into EFS to initiate individuals for the background investigation process:

- Applicant's Name (First, Middle Initial, Last, & Suffix);
- Applicant's Fingerprints;
- Social Security Number (SSN);
- Place of Birth;
- Date of Birth;
- Gender;
- Race;
- Height;
- Weight;
- Eye Color;
- Hair Color;
- Complete Residential Address (Street, City, State, Zip Code, and Country);
- Employing Government Agency, if any; and
- Address of Government Agency, if any.

The following datasets are being requested from IDENT, via CJIS, and returned to FEMA:

- FBI-Known or Appropriately Suspected Terrorist;
- Wants/Warrants;
- FBI/Identification for Firearms Sales;
- FBI-Sex Offender Registry;
- Gang Member;
- Deported Felon;
- Department of Defense (DoD) Lookout;
- Wanted by Interpol;
- Smuggler/Removed Alien;

- Aliens;
- Drugs;
- Final Order (an order to an illegal alien to leave the country); and
- Pending Removal status (pending deportation).

2.2 What are the sources of the information and how is the information collected for the project?

There are three sources of information in EFS – the individual being screened, FBI's CJIS system, and IDENT. FEMA OCSO collects information directly from a current or prospective federal hire, a federal employee, a contractor, or other affiliates, including state, tribal, and local partners, and individuals from voluntary organizations. FEMA collects the information via paper and electronic media. The applicant provides two forms of identification in order for FEMA to verify the identity. All biometric data is captured directly from the individual at the capture station by an electronic fingerprint scanner. The applicant's information is then saved to the FPSF server and transmitted to and searched against the IDENT databases.

FBI data comes from IAFIS. IAFIS is a national fingerprint and criminal history system that responds to requests 24 hours a day, 365 days a year to help local, state, and federal partners solve and prevent crime and catch criminals and terrorists. IAFIS provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses.

IDENT data comes from DHS, collected by, or in cooperation with DHS and its components and may contain information collected by other federal, state, local, tribal, foreign, and international agencies. IDENT is a centralized and dynamic DHS-wide biometric database that also contains limited biographic and encounter history information needed to place the biometric information in proper context.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. FEMA only collects data from the applicant. No other source is needed for the background investigation process.

2.4 Discuss how accuracy of the data is ensured.

Accuracy of the applicant data is confirmed by the identification documents provided by the applicant as the first step in the fingerprinting process. The applicant must provide two acceptable documents listed on the Federal I-9 Form, "List of Acceptable Documents." The applicant is also fingerprinted and the data he or she

provides is confirmed through CJIS and IDENT. If there are any discrepancies in the original information provided from the applicant, FEMA security officials address them in the adjudication process, FEMA OCSO reviews a person's character or conduct over time, resulting in a favorable or unfavorable determination of their employment suitability, eligibility for access to classified information, materials, or areas, or for their retention in federal employment.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that more than the necessary information is collected from the applicants.

Mitigation: This risk is mitigated because FEMA is required to follow specific guidelines regarding the scope of information collected. This is based on information required for background checks in accordance with FEMA policies and standard operating procedures. FEMA OCSO only collects information that is necessary to properly conduct background checks.

Privacy Risk: There is a privacy risk that inaccurate information may impact the suitability status of an applicant.

Mitigation: This risk is mitigated by allowing applicants to review their applications prior to submission. Additionally, the FEMA OCSO Personnel Security Division (PSD) checks and cross references the information received from OPM and the FBI criminal history report to identify any discrepancies in the information. If during the review of this information, the PSD notices inaccurate information or discrepancies between the two sources, and requires further clarification, the PSD will notify the applicant and request supporting or clarifying documentation. For example, if the PSD identifies that the applicant has different Social Security Numbers and addresses listed on the credit history report and criminal history report for the same period of time, the PSD will contact the applicant for clarification. The applicant is then given the opportunity to provide supporting or clarifying documentation to explain the discrepancy (e.g., he or she was a victim of identity theft and has documentation to support this and explain the discrepancy).

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

FEMA OCSO uses the biometric data and PII collected as part of the security suitability, clearance, and badging process. All data collected, including the SSN, is

required by CJIS and OBIM to ensure proper identification and verification of each applicant. The biometric data and PII are entered into IDENT and IAFIS and searched against the databases for possible hits or matches. FEMA OCSO then uses the search results from IDENT and IAFIS to determine the individual's suitability.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, FEMA does not search IDENT for patterns or general terms. Queries are specific to the applicant and only needed for the purpose of the individual's personal background investigation.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. Although data is sent between DHS components (FEMA to NPPD/OBIM via DHS *OneNet*), all users of EFS are within FEMA. There are no other components with assigned roles or responsibilities within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that information is used for unauthorized purposes, or for reasons that are inconsistent with the original purpose of collection.

Mitigation: This privacy risk is mitigated by requiring OBIM, IDENT, and OCSO EFS users, including system administrators, to protect and use data in accordance with the policies, standards, and regulations specified for each system. All system users must read and sign their agency's "Rules of Behavior," statement and comply with DHS and U.S. Government security requirements.

Privacy Risk: There is a privacy risk that unauthorized parties may seek or gain access to the information.

Mitigation: This privacy risk is mitigated by implementing robust technical, management, and operational controls and ensuring sharing protocols are in place to confirm access, which is limited to those with a valid need to know. IDENT and EFS personnel will regularly analyze their respective audit logs to detect and track unusual or suspicious activities across the connection that might indicate intrusions or internal misuse.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

In all cases, EFS provides FEMA applicants, a notice required by the Privacy Act, 5 U.S.C. § 552a(e)(3). All applicants must read and sign a separate Privacy Act notice form. This Privacy Act notice form is provided in both paper and electronic format. The notice states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used.

This PIA and the SORNs listed in 1.2 also serve as notice for information collection. Additionally, all FEMA badging offices display posters with Privacy Act notices to further notify applicants about the collection of information.

FEMA applicants, using an electronic signature process, confirm the presentation of and agree with the Privacy Act Statement, and voluntarily participate in the fingerprinting process and submit to a name-based background check appropriate to job requirements.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals are notified of the uses of their information prior to collection. By confirming and agreeing with the Privacy Act Statement, the individual gives consent to the uses of his or her information. FEMA's OCSO will not use the information outside of the uses and/or scope outlined in this PIA, SORN, and the notice provided on the relevant forms. Should FEMA anticipate a need for a new use for the information, or any major modifications from this initial system accreditation effort resulting in how and/or with whom data is shared, the PIA, SORN, and form notices will be updated.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that inadequate notice is provided leaving individuals unaware of how their information is collected or used.

Mitigation: This privacy risk is mitigated by providing notice to all individuals in the form of a Privacy Act Statement prior to information collection. No use and collection changes will occur without updates to the appropriate documentation. Should FEMA anticipate a need for a new use for the information, or any major modifications

from this initial system accreditation effort resulting in how and/or with whom data is shared the PIA, SORN and form notices will be updated.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 20 through 25, approved by NARA. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

Investigative reports and related documents created or received by FEMA for use in making security/suitability determinations are placed in inactive files after notification of death, separation, or transfer of employee, or expiration of contract relationship. In accordance with NARA Authority N1-311-94-1, Item 1, inactive files are cut off semi-annually and transferred to Federal Records Center (FRC), and destroyed 15 years after cutoff.

Investigative reports and related documents created or received by FEMA for use in making security/suitability determinations that result in substantially actionable issue(s), adverse adjudication, or debarment are placed in inactive files after notification of death, separation, or transfer of employee, or expiration of contract relationship. In accordance with NARA Authority N1-311-94-1, Item 2, inactive files are cut off semi-annually and transferred to FRC, and destroyed 25 years after cutoff.

Data will be retained on the FPSF server for a minimum period of 3 years, not to exceed 7 years.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information is retained longer than required, increasing the amount of harm resulting from an unauthorized disclosure of information.

Mitigation: This privacy risk is mitigated by retaining the information in accordance with the approved NARA retention schedules. A Designated System Administrator is responsible for deleting or archiving information in accordance with the retention schedules. The Designated System Administrator will review all data on an annual basis. Also, security controls are in place to ensure that information is protected during this time.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

EFS sends data to the FBI and OPM for purpose of conducting suitability and security background investigations of employees and contractors.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The purpose of the two SORNs is to collect and maintain biographic and fingerprint information of employees in order to determine suitability, and issue clearances and badging. Primary external sharing is with law enforcement-type entities via routine uses published in DHS/ALL-023 DHS Personnel Security Management SORN, and DHS/ALL-026 Personal Identity Verification Management System SORN. These outside entities receive PII from FEMA and in turn provide valuable data pertaining to an individual's suitability. Thus, any sharing of the PII is compatible with the original purpose for collection.

For example, FEMA shares names and fingerprint information of employees with the FBI which in turn provides FEMA with information as to whether the employees have committed any disqualifying crimes. The FBI is able to retrieve this data based on the information FEMA provides. Without first sharing with the FBI, FEMA would be unable to meet this requirement by law.

FEMA will also share data related to the fingerprints with other appropriate federal, state, local, tribal, foreign, or international agencies, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual and to an individual's prospective or current employer to the extent necessary to determine employment eligibility.

Thus, the sharing is compatible with the purpose of collecting the fingerprint information.

6.3 Does the project place limitations on re-dissemination?

Yes, external agencies are strictly prohibited from sharing the information provided by EFS outside the descriptions in this PIA. These limitations are understood

and acknowledged by the EFS Rules of Behavior. The EFS System Owner receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the Rules of Behavior, before authorizing access to information and the information system. All EFS users are required to sign Rules of Behavior prior to being granted system accounts or access to the EFS systems or data. The Rules of Behavior shall contain a "Consent to Monitor" provision and an acknowledgement that the user has no expectation of privacy in his or her use of the system.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

As identified in the SORNs listed in 1.2, requests for records from FEMA/OCSO are made to the FEMA Disclosure Office, which maintains the accounting of what records were disclosed and to whom.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that information may be disclosed or inappropriately shared with unauthorized entities.

Mitigation: This privacy risk is mitigated by only disclosing information pursuant to the routine uses of the SORNs listed in 1.2. FEMA has a Memorandum of Understanding (MOU) in place with OPM to ensure that there are formal procedures in place to secure and protect FEMA employee and contractor data. OPM is required not only by the MOU with FEMA but also by government-wide security standards to ensure that any information it receives or transmits is transmitted to a party which has a need to know and that the receiving party has adequate security measures in place.

Privacy Risk: There is a privacy risk of unauthorized disclosure of information during electronic capture/transmission of fingerprints from EFS to OPM.

Mitigation: To mitigate the risk of unauthorized disclosure when transmitting data electronically, DHS and OPM have taken necessary and reasonable measures to ensure that such events do not take place, such as trusted Virtual Protected Network (VPN) tunnels, data encryption, and additional security measures.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals may directly correct basic information such as address and phone number at any time after the clearance process is completed. This will be completed through a DHS website with manager approval of each change. During the clearance process individuals may not alter their information. They may inform the FEMA OCSO of a change in their information, but may not directly access it.

Individuals may consult the SORNs for additional information regarding how to access their information via Privacy Act or Freedom of Information Act (FOIA) request submitted to the FEMA Disclosure Office. Such requests should be sent to: FEMA Disclosure Officer, Records Management Division, 500 C Street, SW, Washington, DC 20472.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Once the information provided by the applicant during the pre-enrollment and enrollment processes has been verified and authenticated, changes to the database would occur for a name change or for additional information provided through adjudication procedures. Individuals may directly correct basic information such as address and phone number at any time after the clearance process is completed.

Furthermore, the SORNs listed in Section 1.2 and this PIA also provide notice on how individuals can access and correct their information.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are informed in writing and given an opportunity to explain, refute, or deny the information in their background check. If during this process, FEMA identifies any discrepancies in the information (e.g., inaccurate information, adverse information), FEMA contacts the individual and provides the individual an opportunity to provide mitigating or clarifying documentation. If the adverse information is appropriately mitigated, then he or she is approved in writing for suitability or security clearance in addition to being eligible for clearance. Additionally, during the enter on duty process and before receiving clearance, the form used for issuance of the actual card contains notice reminding the employee or contractor of the ability to access information as well as notice of the uses of the collection.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that inaccurate information may be used to make a determination on the individual's suitability.

Mitigation: To mitigate this privacy risk, prior to FEMA OCSO making a determination on an individual's suitability for employment or ineligibility for a clearance, based on adverse information obtained in his or her background investigation (including criminal history and credit checks), the individual will be afforded his or her rights as outlined in the law and DHS policies. For example, an individual is given the opportunity to clarify or provide supporting or mitigating documentation for any discrepancies found in the credit history report and criminal history reports.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

EFS uses a separation of access capabilities based on process roles. FEMA OCSO ensures access to employee information is both restricted and controlled. An internal audit process will be defined and implemented within 12 months of ATO. Audit logs will be established and regularly verified to ensure the possibility of a breach is minimized, and include automated tools to indicate when information is possibly being misused.

Should a breach occur FEMA OCSO has a plan in place to immediately respond to the breach. Self-audits, third party audits, and reviews by the Office of Inspector General or Government Accountability Office will be performed as needed or as required by law. Attempts to access sensitive data are recorded for forensic purposes if an unauthorized individual attempts to access the information contained within the system.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

FEMA employees (including EFS users and administrators) are required to complete annual privacy and security training. If any FEMA employee fails to complete the required annual training, access to FEMA networks and facilities is denied until mandatory training requirements are fulfilled. FEMA OCSO has implemented strict guidelines, and enforces adherence for its employees as it pertains to protecting personal and sensitive employee information.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Authorized FEMA OCSO personnel or contractors (pursuant to an appropriate routine use) who handle the operations and maintenance of the system will have position-specific access to the system to support the primary system function, as well as, troubleshoot technical system issues encountered on a day-to-day basis. All assigned FEMA employees and contractor staff will receive appropriate privacy and security training and have any necessary background investigations and/or security clearances for access to sensitive, private, or classified information and secured facilities. FEMA ensures this through legal agreements with its contractors and enforcement of internal procedures with all DHS entities involved in processing the background checks. Additionally, robust standard operation procedures and system user manuals describe user roles, responsibilities, and access privileges.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

FEMA's process for reviewing and approving MOUs and ISAs involve FEMA's IT Security Branch, FEMA Privacy Officer, and the Office of Chief Counsel, as well as the appropriate authorities from the other agency/organization to the agreement. FEMA will review these agreements on an annual basis and review appropriate security documents for any newly identified risks. FEMA will mitigate any newly identified risks between the partnering agencies in accordance with applicable laws.

Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
U.S. Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security